UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF ILLINOIS
EASTERN DIVISION

SHANNAN ELLIS, RICH FREIBERG, CHRISTOPHER ROY, and STEPHEN RIES, individually and on behalf of all others similarly situated, Plaintiffs, vs. HUB INTERNATIONAL LIMITED, Defendant.	Case No. 1:23-cv-06137 Hon. John J. Tharp Jr. **JURY TRIAL DEMANDED**

CONSOLIDATED CLASS ACTION COMPLAINT

Plaintiffs Shannan Ellis, Rich Freiberg, Christopher Roy, and Stephen Ries ("Plaintiffs") bring this action, on behalf of themselves and all others similarly situated, against Defendant HUB International Limited ("HUB" or "Defendant"), and allege as follows:

I. INTRODUCTION

1. This lawsuit stems from a massive and preventable data breach spanning from December 2022 through January 2023 in which cybercriminals infiltrated HUB's inadequately protected network systems and accessed the highly sensitive personally identifiable information ("PII") of approximately **479,261 individuals** (the "Data Breach" or Breach").[1]

2. According to HUB, the Data Breach began in or around December 2022, but was not discovered by HUB until January 17, 2023.[2]

[1] *See* https://apps.web.maine.gov/online/aeviewer/ME/40/a5e4c9cb-5a57-4d11-aa3a-88c06e7a220d.shtml (last accessed Oct. 5, 2023).

[2] *See* https://apps.web.maine.gov/online/aeviewer/ME/40/a5e4c9cb-5a57-4d11-aa3a-

3. After an investigation, HUB determined that the types of PII accessed and copied by cybercriminals during the Data Breach included, *inter alia*, names, Social Security numbers, driver's license numbers, passport numbers, and financial account information ("Personal Information" or "Private Information").[3]

4. On August 11, 2023 (seven months after the unauthorized party first gained access to Plaintiffs' and the Class's PII), victims of the Data Breach were finally notified via letter that their highly sensitive and confidential PII was exposed in a data breach ("Notice of Data Breach Letter" or "Notice").[4]

5. The Notice of Data Breach Letter obscured the nature of the Breach and the threat it posed, failing to notify Plaintiffs and the Class how many people were impacted, how the Breach happened, or why it took so long to begin notifying victims that hackers had gained access to their highly sensitive PII.

6. Defendant's failure to timely detect and report the Data Breach made the victims vulnerable to identity theft without any warnings to monitor their financial accounts or credit reports to prevent unauthorized use of their PII.

7. Defendant knew or should have known that each victim of the Data Breach deserved prompt and efficient notice of the Data Breach and assistance in mitigating the effects of PII misuse.

88c06e7a220d/cbae5041-4b0b-4eea-847a-a514f26ce92d/document.html (last accessed Oct. 5, 2023).

[3] *Id.*; *see also* https://dataconomy.com/2023/08/15/hub-international-data-breach/ (last accessed Oct. 5, 2023).

[4] *See* https://apps.web.maine.gov/online/aeviewer/ME/40/a5e4c9cb-5a57-4d11-aa3a-88c06e7a220d/cbae5041-4b0b-4eea-847a-a514f26ce92d/document.html.

8. In failing to adequately protect Plaintiffs' and the Class's PII, failing to adequately notify them of the Breach, and by obfuscating the nature of the Breach, Defendant violated state and federal laws and harmed Plaintiffs and the Class.

9. Plaintiffs and members of the Class are victims of Defendant's negligence and inadequate cyber security measures.

10. HUB failed to implement industry standard data security practices to prevent the Data Breach.

11. Upon information and belief, the unauthorized third-party cybercriminals gained access to Plaintiffs' and Class Members' PII with the intent of engaging in misuse of said PII, including marketing and selling Plaintiffs' and Class Members' PII on the dark web, a known marketplace for criminal activity.

12. Today, the identities of Plaintiffs and Class Members are in jeopardy, all because of Defendant's negligence. Plaintiffs and Class Members now suffer from a heightened and imminent risk of fraud and identity theft and must now constantly monitor their financial accounts.

13. Accordingly, Plaintiffs, on their own behalf and on behalf of a class of similarly situated individuals, brings this lawsuit seeking injunctive relief, damages, and restitution, together with costs and reasonable attorneys' fees, the calculation of which will be based on information in Defendant's possession.

II. PARTIES

14. Plaintiff **Shannan Ellis** is a natural person and citizen of Minnesota. Plaintiff has no intention to move within the next two years.

15. Plaintiff **Rich Freiberg** is a natural person and citizen of North Carolina.

Plaintiff has no intention to move within the next two years.

16. Plaintiff **Christopher Roy** is a natural person and citizen of Massachusetts. Plaintiff has no intention to move within the next two years.

17. Plaintiff **Stephen Ries** is a natural person and citizen of North Dakota. Plaintiff has no intention to move within the next two years.

18. Defendant **HUB** is a Delaware corporation registered as a foreign corporation in the State of Illinois. HUB's headquarters and principal place of business is located at 150 N. Riverside Plaza, 17th Floor, Chicago, IL 60606.

III. JURISDICTION & VENUE

19. This Court has subject matter jurisdiction over this action under 28 U.S.C.§ 1332(d) because this is a class action wherein the amount in controversy exceeds the sum or value of $5,000,000, exclusive of interest and costs, there are more than 100 members in the proposed class, and Plaintiffs (and many members of the Class) and Defendant are citizens of different states.

20. This Court has personal jurisdiction over Defendant because Defendant maintains its principal place of business in this District and does substantial business in this District.

21. Venue is proper in this District under 28 U.S.C. § 1391(b)(2) because a substantial part of the events or omissions giving rise to the claim occurred in this District.

IV. FACTUAL ALLEGATIONS

Defendant's Business and the Collection of Plaintiffs' and the Class's PII

22. HUB is an insurance brokerage company based in Chicago, Illinois.[5]

[5] https://www.jdsupra.com/legalnews/hub-international-limited-files-notice-7826466/ (last

23. HUB provides various types of insurance through its marketplace, including property, casualty, risk management, life and health reinsurance, and employee benefits services.[6]

24. According to HUB's website, HUB generates approximately $3.7 billion in annual revenue and has an estimated overall business value of $23 billion.

25. As such, HUB had more than sufficient funds to implement adequate data security infrastructure, training, procedures, and protocols.[7]

26. To operate its business, HUB creates, collects, and stores customers' and policy holders' Personal Information. Stated another way, HUB requires its customers and policyholders to disclose their Personal Information to receive HUB's services, including, among other things, their Private Information.

27. Plaintiffs and the Class are customers and/or policyholders of Defendant and were required to disclose their Private Information to HUB to receive services. Thus, Defendant was in possession of Plaintiffs' and the Class's PII before, during, and after the Data Breach.

28. By collecting and maintaining Plaintiffs' and the Class's PII, Defendant implicitly agreed it would protect and safeguard the PII it collected and maintained from Plaintiffs and the Class by complying with state and federal laws, regulations, and applicable industry standards.

---

accessed Oct. 5, 2023).

[6] *Id.*

[7] https://www.hubinternational.com/media-center/press-releases/2023/04/hub-internationals-market-leading-position-attracts-investment-by-leonard-green/#:~:text=In%202022%2C%20HUB%20hit%20%243.7,ability%20to%20persevere%20and%20excel.

29. Additionally, upon information and belief, HUB represented to its employees, customers, policyholders, and members orally and in written contracts, marketing materials, and otherwise that it would properly protect all PII it obtained. HUB knew or reasonably should have known that such representations would be passed on to the public including Plaintiffs and Class Members.

30. It is apparent from HUB's public representations that at all times relevant, HUB understood the importance of protecting Plaintiffs' and the Class's Private Information and its duty to protect and secure the Private Information it collected and maintained.

31. For example, HUB represents on its website, "[w]e generally only disclose your Personal Information to perform services on your behalf and provide you with the insurance products and services you expect from us."[8]

32. HUB's Privacy Policy ("Privacy Policy"), states , "[w]e maintain technical and organizational security measures reasonably designed to protect the security of your Personal Information against loss, misuse, unauthorized access, disclosure, or alteration. HUB International Limited and its affiliates take steps in accordance with the Systems Information and Standards of our Code of Business Conduct and Ethics to secure your Personal Information with appropriate levels of security around storage and use."[9]

33. Further, HUB's Privacy Policy also states, "[i]n the event of a breach impacting your Personal Information, we intend to provide you with notification to the extent required by applicable law."[10]

---

[8] https://www.hubinternational.com/about-us/privacy-policy/ (last accessed Oct. 5, 2023).

[9] *Id.*

[10] *Id.*

34. Despite recognizing the importance of data security, HUB utterly failed to adequately secure and protect the highly sensitive Private Information of Plaintiffs and the Class.

The Data Breach

35. According to HUB, on January 17, 2023, HUB "identified suspicious activity on certain systems within its network."[11]

36. Following an internal investigation, HUB discovered "certain systems within [its] network were accessed by an unknown individual and files were copied without authorization between December 2022 and January 2023."[12]

37. By virtue of the above statement, HUB openly admits that not only was the Private Information of Plaintiffs and the Class ***accessed*** by an unauthorized individual, but the Private Information of Plaintiffs and the Class was ***stolen***.

38. The types of Private Information stolen in the Data Breach included: *inter alia*, names, Social Security numbers, driver's license numbers, passport numbers, and financial account information.

39. As a result of the Data Breach, Plaintiffs' and the Class's personal and highly sensitive information was stolen and is in the hands of cybercriminals who will place their sensitive PII for sale on the dark web or use their PII to perpetrate identity theft—if they have not done so already.

40. Upon information and belief, the unauthorized third-party cybercriminals gained access to Plaintiffs' and Class Members' PII with the intent of engaging in misuse of the PII,

[11] *See* https://apps.web.maine.gov/online/aeviewer/ME/40/a5e4c9cb-5a57-4d11-aa3a-88c06e7a220d/cbae5041-4b0b-4eea-847a-a514f26ce92d/document.html.

[12] *Id.*

including marketing and selling Plaintiffs' and Class Members' PII.

41. All in all, HUB's cyber and data security systems were completely inadequate and allowed cybercriminals to obtain files containing a treasure trove of thousands of individuals' highly sensitive PII, including that of Plaintiffs and the Class.

42. On or around August 11, 2023—months after the Breach occurred—Plaintiffs and Class Members were finally notified of the Data Breach via Notice of Data Breach Letters.[13]

43. In the Notice of Data Breach Letters sent to Plaintiffs and the Class, HUB deliberately failed to disclose the exact dates of the Data Breach, including when the Data Breach began and when it ended.

44. In the Notice of Data Breach Letter, HUB also failed to make any assurances that it recovered Plaintiffs' and the Class's stolen Private Information.

45. Instead, HUB acknowledged the certainly impending risk of harm Plaintiffs and the Class now face by offering them twelve months of credit monitoring identity theft protection services. However, such an offering is inadequate as Plaintiffs and the Class will need these services for the rest of their lives.

46. Defendant also recognized the actual imminent harm and injury that flowed from the Data Breach by encouraging Data Breach victims to "remain vigilant against incidents of identity theft and fraud by reviewing your account statements and monitoring your free credit reports" and to take the following steps:

a. order your free credit report;

[13] https://apps.web.maine.gov/online/aeviewer/ME/40/a5e4c9cb-5a57-4d11-aa3a-88c06e7a220d/cbae5041-4b0b-4eea-847a-a514f26ce92d/document.html.

b. if you believe you are the victim of identity theft or have reason to believe your personal information has been misused, contact the FTC and/or your state's attorney general office about for information on how to prevent or avoid identity theft;

c. place a security freeze; and

d. place a fraud alert.[14]

47. HUB largely put the burden on Plaintiffs and Class Members to take measures to protect themselves.

48. Time is a compensable and valuable resource in the United States. According to the U.S. Bureau of Labor Statistics, 55.5% of U.S.-based workers are compensated on an hourly basis, while the other 44.5% are salaried.[15]

49. According to the U.S. Bureau of Labor Statistics' 2018 American Time Use Survey, American adults have only 36 to 40 hours of "leisure time" outside of work per week;[16] leisure time is defined as time not occupied with work or chores and is "the time equivalent of 'disposable income.'"[17] Usually, this time can be spent at the option and choice of the consumer,

---

[14] *Id.*

[15] *Characteristics of minimum wage workers, 2020*, U.S. BUREAU OF LABOR STATISTICS https://www.bls.gov/opub/reports/minimum-wage/2020/home.htm#:~:text=In%202020%2C%2073.3%20million%20workers,wage%20of%20%247.25%20per%20hour (last accessed Oct. 21, 2022); *Average Weekly Wage Data*, U.S. BUREAU OF LABOR STATISTICS, *Average Weekly Wage Data,* https://data.bls.gov/cew/apps/table_maker/v4/table_maker.htm%23type=1&year=2021&qtr=3&own=5&ind=10&supp=0 (last accessed Aug. 2, 2022) (finding that on average, private-sector workers make $1,253 per 40-hour work week.).

[16] Cory Stieg, *You're spending your free time wrong — here's what to do to be happier and more successful*, CNBC https://www.cnbc.com/2019/11/06/how-successful-people-spend-leisure-time-james-wallman.html (Nov. 6, 2019).

[17] *Id.*

however, having been notified of the Data Breach, consumers now have to spend hours of their leisure time self-monitoring their accounts, communicating with financial institutions and government entities, and placing other prophylactic measures in place to attempt to protect themselves.

50. Plaintiffs and Class Members are now deprived of the choice as to how to spend their valuable free hours and seek renumeration for the loss of valuable time as another element of damages.

51. In response to the Data Breach, HUB contends it has or will be taking steps to address the Data Breach.[18] Although HUB failed to expound on what these alleged "steps" are, such steps should have been in place before the Data Breach.

HUB's Failures Causing the Data Breach

52. Despite HUB's duties to safeguard Plaintiffs' and the Class's PII, HUB did not follow industry standard practices in securing Plaintiffs' and the Class's PII, as evidenced by the Data Breach.

53. Despite the prevalence of public announcements of data breaches and data security compromises, HUB failed to take appropriate steps to protect Plaintiffs' and Class Members' PII from being compromised.

54. HUB failed to ensure the proper monitoring and logging of the ingress and egress of network traffic.

55. HUB failed to ensure the proper monitoring and logging of file access and modifications.

56. HUB failed to ensure the proper encryption of Plaintiffs' and Class Members' PII.

[18] *Id.*

57. HUB knowingly disregarded standard information security principles, despite obvious risks, by allowing unmonitored and unrestricted access to unsecured PII.

58. HUB failed to ensure the proper implementation of sufficient processes to quickly detect and respond to data breaches, security incidents, or intrusions.

59. HUB failed to provide adequate supervision and oversight of the PII with which it was and is entrusted, in spite of the known risk and foreseeable likelihood of breach and misuse, which permitted an unknown third party to gather PII of Plaintiffs and Class Members, misuse the PII and potentially disclose it to others without consent.

The Data Breach was a Foreseeable Risk of which Defendant were on Notice.

60. Defendant's data security obligations were particularly important given the substantial increase in cyberattacks and/or data breaches in similar industries preceding the date of the breach.

61. In light of recent high profile data breaches, Defendant knew or should have known that their electronic records and Plaintiffs and the Class's PII would be targeted by cybercriminals.

62. In 2021, a record 1,862 data breaches occurred, resulting in approximately 293,927,708 sensitive records being exposed, a 68% increase from 2020.[19] The 330 reported breaches reported in 2021 exposed nearly 30 million sensitive records (28,045,658), compared to only 306 breaches that exposed nearly 10 million sensitive records (9,700,238) in 2020.[20]

---

[19] 2021 Data Breach Annual Report, ITRC, chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.wsav.com/wp-content/uploads/sites/75/2022/01/20220124_ITRC-2021-Data-Breach-Report.pdf.

[20] *Id.*

63. Indeed, cyberattacks against have become increasingly common for over ten years, with the FBI warning as early as 2011 that cybercriminals were "advancing their abilities to attack a system remotely" and "[o]nce a system is compromised, cyber criminals will use their accesses to obtain PII." The FBI further warned that that "the increasing sophistication of cyber criminals will no doubt lead to an escalation in cybercrime."[21]

64. Therefore, the increase in such attacks, and attendant risk of future attacks, was widely known to the public and to anyone in Defendant's industry, including HUB.

The Experiences and Injuries of Plaintiffs and Class Members

65. Plaintiffs and Class Members are former and current customers of HUB.

66. Plaintiffs and Class Members provided valuable consideration—a portion of which was intended to have been used by HUB to secure Plaintiffs' and Class Members' PII—to HUB in exchange for its services.

67. As a prerequisite of receiving its services, HUB requires its customers—like Plaintiffs and Class Members—to disclose their PII to HUB.

68. Because of the Data Breach, HUB inflicted injuries upon Plaintiffs and Class Members. And yet, HUB has done little to provide Plaintiffs and Class Members with relief for the damages they suffered.

69. Plaintiffs and Class Members entrusted their PII to HUB. Thus, Plaintiffs and Class Members had the reasonable expectation and mutual understanding that HUB would take—at minimum—industry standard precautions to protect, maintain, and safeguard that information from unauthorized users or disclosure, and would timely notify them of any data security incidents.

[21] Gordon M. Snow Statement, FBI https://archives.fbi.gov/archives/news/testimony/cyber-security-threats-to-the-financial-sector.

After all, Plaintiffs and Class Members would not have entrusted their PII to HUB had they known that HUB would not take reasonable steps to safeguard their information.

70. Plaintiffs and Class Members suffered actual injury from having their PII compromised in the Data Breach including, but not limited to, (a) damage to and diminution in the value of their PII—a form of property that HUB obtained from Plaintiffs and Class Members; (b) violation of their privacy rights; (c) the likely theft of their PII; (d) fraudulent activity resulting from the Breach; and (e) present and continuing injury arising from the increased and imminent risk of additional identity theft and fraud.

71. As a result of the Data Breach, Plaintiffs and Class Members also suffered emotional distress because of the release of their PII, which they believed would be protected from unauthorized access and disclosure. Now, Plaintiffs and Class Members suffer from anxiety about unauthorized parties viewing, selling, and/or using their PII for nefarious purposes like identity theft and fraud.

72. Because of the Data Breach, Plaintiffs and Class Members have spent—and will continue to spend—considerable time and money to try to mitigate and address harms caused by the Data Breach.

Plaintiff Ellis's Experience

73. Plaintiff Ellis received a Notice of Data Breach Letter, dated August 11, 2023, notifying her that her that some of her Private Information was identified by HUB as being "accessed" and "copied" by an unauthorized actor between December 2022 and January 2023. Specifically, the Notice of Data Breach Letter informed Plaintiff Ellis that her Social Security number was compromised in the Data Breach.

74. As a result of the Data Breach and at the recommendation of HUB, Plaintiff Ellis

spent hours dealing with the consequences of the Data Breach, which includes time spent verifying the legitimacy of the Notice of Data Breach Letter, self-monitoring her accounts, and monitoring her credit reports for suspicious and fraudulent activity. This time has been lost forever and cannot be recaptured. Plaintiff Ellis has spent and will continue to spend considerable time and effort monitoring her accounts to protect herself from identity theft for the rest of her life.

75. After the Data Breach, Plaintiff Ellis purchased an annual subscription to LifeLock™ for $239.88 to monitor her Private Information that HUB allowed cybercriminals to access and steal. However, this is not a one-time expense. When Plaintiff Ellis's LifeLock™ subscription renews on October 9, 2024, Plaintiff Ellis's rate will increase to $339.99 per year (not including applicable tax). Plaintiff Ellis will continue to need credit monitoring and identity theft protection services such as LifeLock™ for the rest of her life and will be forced to purchase these services on an annual basis.

76. Additionally, after the Data Breach Plaintiff Ellis experienced fraudulent charges to her Wells Fargo credit card totaling over $1,000.00 during March 2023 and April 2023.[22] Plaintiff alleges these instances of fraud are fairly traceable to the Data Breach.

77. Plaintiff Ellis fears for her personal financial security and uncertainty over what PII was exposed in the Data Breach. Particularly, Plaintiff Ellis has and is experiencing feelings of anxiety, sleep disruption, stress, fear, and frustration because of the Data Breach. This goes far beyond allegations of mere worry or inconvenience; it is exactly the sort of injury and harm to a Data Breach victim that the law contemplates and addresses. These feelings of anxiety are exacerbated by the fact that her children have monetary accounts tied to her PII as well. Thus,

[22] "An identity thief can use your SSN together with your PII to open new bank accounts **or access existing ones**, take out credit cards, and apply for loans all in your name." https://surfshark.com/blog/what-can-someone-do-with-your-ssn (emphasis added).

Plaintiff Ellis is not only concerned about her own future financial harm, but that of her children as well.

78. Plaintiff Ellis suffered actual injury as a result of the Data Breach in the form of (a) damage to and diminution in the value of her PII, a form of intangible property that Defendant obtained from Plaintiff Ellis; (b) violation of her privacy rights; and (c) present, imminent, and impending injury arising from the increased risk of identity theft, and fraud she now faces.

79. Plaintiff Ellis has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from her PII being placed in the hands of unauthorized third parties and possibly criminals.

80. Plaintiff Ellis has a continuing interest in ensuring that her PII, which, upon information and belief, remains backed up in Defendant's possession, is protected, and safeguarded from future breaches.

Plaintiff Freiberg's Experience

81. Plaintiff Freiberg received a Notice of Data Breach Letter, dated August 11, 2023, notifying him that his PII was identified by HUB as being "accessed" and "copied" by an unauthorized actor between December 2022 and January 2023. Specifically, the letter notified him that his Social Security number and driver's license number was compromised in the Data Breach

82. As a result of the Data Breach and at the recommendation of HUB, Plaintiff Freiberg spent hours dealing with the consequences of the Data Breach, which includes time spent verifying the legitimacy of the Notice of Data Breach Letter, self-monitoring his accounts, and monitoring his credit reports for suspicious and fraudulent activity. This time has been lost forever and cannot be recaptured. Plaintiff Freiberg has spent and will continue to spend considerable time and effort monitoring his accounts to protect himself from identity theft for the rest of his life.

83. Plaintiff Freiberg suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach and has experienced anxiety and increased concerns for the loss of his privacy, as well as anxiety over the impact of cybercriminals accessing and using his PII.

84. Plaintiff Freiberg suffered actual injury as a result of the Data Breach in the form of (a) damage to and diminution in the value of his PII, a form of intangible property that Defendant obtained from Plaintiff Freiberg; (b) violation of his privacy rights; and (c) present, imminent, and impending injury arising from the increased risk of identity theft, and fraud he now faces.

85. Plaintiff Freiberg is now subject to the present and continuing risk of fraud, identity theft, and misuse resulting from his PII, in combination with his name, being placed in the hands of unauthorized third parties/criminals. This risk is substantial and imminent in light of the fraudulent misuse of the compromised PII that has already impacted the lives of other Class Members.

86. Plaintiff Freiberg has a continuing interest in ensuring that his PII, which, upon information and belief, remains backed up in HUB's possession, is protected and safeguarded from future breaches.

Plaintiff Roy's Experience

87. Plaintiff Roy received a Notice of Data Breach Letter, dated August 11, 2023, notifying him that his PII was identified by HUB as being "accessed" and "copied" by an unauthorized actor between December 2022 and January 2023. Specifically, the letter notified him that his driver's license and date of birth were compromised in the Data Breach.

88. As a result of the Data Breach and at the recommendation of HUB, Plaintiff Roy spent hours dealing with the consequences of the Data Breach, which includes time spent verifying the legitimacy of the Notice of Data Breach Letter, self-monitoring his accounts, and monitoring

his credit reports for suspicious and fraudulent activity. This time has been lost forever and cannot be recaptured. Plaintiff Roy has spent and will continue to spend considerable time and effort monitoring his accounts to protect himself from identity theft for the rest of his life.

89. Plaintiff Roy suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach and has experienced anxiety and increased concerns for the loss of his privacy, as well as anxiety over the impact of cybercriminals accessing and using his PII.

90. Plaintiff Roy suffered actual injury as a result of the Data Breach in the form of (a) damage to and diminution in the value of his PII, a form of intangible property that Defendant obtained from Plaintiff Roy; (b) violation of his privacy rights; and (c) present, imminent, and impending injury arising from the increased risk of identity theft, and fraud he now faces.

91. Plaintiff Roy is now subject to the present and continuing risk of fraud, identity theft, and misuse resulting from his PII, in combination with his name, being placed in the hands of unauthorized third parties/criminals. This risk is substantial and imminent in light of the fraudulent misuse of the compromised PII that has already impacted the lives of other Class Members.

92. Plaintiff Roy has a continuing interest in ensuring that his PII, which, upon information and belief, remains backed up in HUB's possession, is protected and safeguarded from future breaches.

Plaintiff Ries's Experience

93. Plaintiff Ries received a Notice of Data Breach Letter, dated August 11, 2023, notifying him that his PII was identified by HUB as being "accessed" and "copied" by an unauthorized actor between December 2022 and January 2023. Specifically, the letter notified him that his Social Security number driver's license number had been compromised in the Data Breach.

94. As a result of the Data Breach and at the recommendation of HUB, Plaintiff Ries spent hours dealing with the consequences of the Data Breach, which includes time spent verifying the legitimacy of the Notice of Data Breach Letter, self-monitoring his accounts, and monitoring his credit reports for suspicious and fraudulent activity. This time has been lost forever and cannot be recaptured. Plaintiff Ries has spent and will continue to spend considerable time and effort monitoring his accounts to protect himself from identity theft for the rest of his life.

95. Plaintiff Ries suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach and has experienced anxiety and increased concerns for the loss of his privacy, as well as anxiety over the impact of cybercriminals accessing and using his PII.

96. Plaintiff Ries suffered actual injury as a result of the Data Breach in the form of (a) damage to and diminution in the value of his PII, a form of intangible property that Defendant obtained from Plaintiff Ries; (b) violation of his privacy rights; and (c) present, imminent, and impending injury arising from the increased risk of identity theft, and fraud he now faces.

97. Plaintiff Ries is now subject to the present and continuing risk of fraud, identity theft, and misuse resulting from his PII, in combination with his name, being placed in the hands of unauthorized third parties/criminals. This risk is substantial and imminent in light of the fraudulent misuse of the compromised PII that has already impacted the lives of other Class Members.

98. Plaintiff Ries has a continuing interest in ensuring that his PII, which, upon information and belief, remains backed up in HUB's possession, is protected and safeguarded from future breaches.

Plaintiffs and the Proposed Class Face Significant Risk of Continued Identity Theft

99. Plaintiffs members of the Class have suffered injury from the theft of their PII

that can be directly traced to Defendant.

100. Stolen PII is one of the most valuable commodities on the criminal information black market. According to Experian, a credit-monitoring service, stolen PII can be worth up to $1,000.00 depending on the type of information obtained.

101. The value of Plaintiffs' and the Class's PII on the black market is considerable. Stolen PII trades on the black market for years, and criminals frequently post stolen PII openly and directly on various "dark web" internet websites, making the information publicly available, for a substantial fee of course.

102. It can take victims years to spot identity theft, giving criminals plenty of time to use that information for cash.

103. One such example of criminals using PII for profit is the development of "Fullz" packages.

104. Cyber-criminals can cross-reference two sources of PII to marry unregulated data available elsewhere to criminally stolen data with an astonishingly complete scope and degree of accuracy in order to assemble complete dossiers on individuals. These dossiers are known as "Fullz" packages.

105. The development of "Fullz" packages means that stolen PII from the Data Breach can easily be used to link and identify it to Plaintiffs and the proposed Class's phone numbers, email addresses, and other unregulated sources and identifiers. In other words, even if certain information such as emails, phone numbers, or credit card numbers may not be included in the PII stolen by the cyber-criminals in the Data Breach, criminals can easily create a Fullz package and sell it at a higher price to unscrupulous operators and criminals (such as illegal and scam telemarketers) over and over. That is exactly what is happening to Plaintiffs and members of the

proposed Class, and it is reasonable for any trier of fact, including this Court or a jury, to find that Plaintiffs' and the Class's stolen PII is being misused, and that such misuse is fairly traceable to the Data Breach.

106. Defendant disclosed the PII of Plaintiffs and the Class for criminals to use in the conduct of criminal activity. Specifically, Defendant opened up, disclosed, and exposed the PII of Plaintiffs and the Class to people engaged in disruptive and unlawful business practices and tactics, including online account hacking, unauthorized use of financial accounts, and fraudulent attempts to open unauthorized financial accounts (i.e., identity fraud), all using the stolen PII.

107. Defendant's failure to properly notify Plaintiffs and members of the Class of the Data Breach exacerbated Plaintiffs' and the Class's injury by depriving them of the earliest ability to take appropriate measures to protect their PII and take other necessary steps to mitigate the harm caused by the Data Breach.

108. As a result of Defendant's failure to prevent the Data Breach, Plaintiffs and the Class have suffered and will continue to suffer damages, including monetary losses, lost time, anxiety, and emotional distress. They have suffered or are at an increased risk of suffering:

a. The loss of the opportunity to control how their PII is used;

b. The diminution in value of their PII;

c. The compromise and continuing publication of their PII;

d. out-of-pocket costs associated with the prevention, detection, recovery, and remediation from identity theft or fraud;

e. Lost opportunity costs and lost wages associated with the time and effort expended addressing and attempting to mitigate the actual and future consequences of the Data Breach, including, but not limited to, efforts spent

researching how to prevent, detect, contest, and recover from identity theft and fraud;

f. Delay in receipt of tax refund monies;

g. Unauthorized use of stolen PII; and

h. The continued risk to their PII, which remains in Defendant's possession and is subject to further breaches so long as Defendant fails to undertake the appropriate measures to protect the PII in their possession.

Defendant failed to adhere to FTC guidelines.

109. According to the Federal Trade Commission ("FTC"), the need for data security should be factored into all business decision-making. To that end, the FTC has issued numerous guidelines identifying best data security practices that businesses, such as Defendant, should employ to protect against the unlawful exposure of PII.

110. In 2016, the FTC updated its publication, Protecting PII: A Guide for Business, which established guidelines for fundamental data security principles and practices for business. The guidelines explain that businesses should:

a. protect the sensitive consumer information that they keep;

b. properly dispose of PII that is no longer needed;

c. encrypt information stored on computer networks;

d. understand their network's vulnerabilities; and

e. implement policies to correct security problems.

111. The guidelines also recommend that businesses watch for large amounts of data being transmitted from the system and have a response plan ready in the event of a breach.

112. The FTC recommends that companies not maintain information longer than is

needed for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.

113. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect consumer data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

114. Defendant's failure to employ reasonable and appropriate measures to protect against unauthorized access to employees' PII constitutes an unfair act or practice prohibited by Section 5 of the FTCA, 15 U.S.C. § 45.

V. CLASS ACTION ALLEGATIONS

115. Pursuant to Federal Rule of Civil Procedure 23(b)(2) and (b)(3), Plaintiffs sue on behalf of themselves and the proposed class defined as follows (the "Class"):

> **All individuals residing in the United States whose PII was compromised in the Data Breach discovered by HUB on or around January 17, 2023, or who were sent a Notice of Data Breach Letter.**

Excluded from the Class are Defendant, its agents, affiliates, parents, subsidiaries, any entity in which Defendant has a controlling interest, any of Defendant's officers or directors, any successors, and any Judge who adjudicates this case, including their staff and immediate family.

116. Plaintiffs reserve the right to amend the class definitions.

117. This action satisfies the numerosity, commonality, typicality, and adequacy requirements under Fed. R. Civ. P. 23.

f. **Numerosity**. Plaintiffs are representatives of the Class, consisting of at least **479,261 individuals**, far too many to join in a single action;

g. **Ascertainability**. Members of the Class are readily identifiable from information in Defendant's possession, custody, and control;

h. **Typicality**. Plaintiffs' claims are typical of class claims as each arises from the same Data Breach, the same alleged violations by Defendant, and the same unreasonable manner of notifying individuals about the Data Breach.

i. **Adequacy**. Plaintiffs will fairly and adequately protect the proposed Class's interests. Plaintiffs' interests do not conflict with the Class's interests, and Plaintiffs have retained counsel experienced in complex class action litigation and data privacy to prosecute this action on the Class's behalf, including lead counsel.

j. **Commonality**. Plaintiffs' and the Class's claims raise predominantly common fact and legal questions that a class wide proceeding can answer for the Class. Indeed, it will be necessary to answer the following questions:

i. Whether Defendant had a duty to use reasonable care in safeguarding Plaintiffs' and the Class's PII;

ii. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

iii. Whether Defendant was negligent in maintaining, protecting, and securing PII;

iv. Whether Defendant breached contract promises to safeguard Plaintiffs' and the Class's PII;

v. Whether Defendant took reasonable measures to determine the extent of the Data Breach after discovering it;

vi. Whether Defendant's Breach Notice was reasonable;

vii. Whether the Data Breach caused Plaintiffs' and the Class's injuries;

viii. What the proper measure of damages is; and

ix. Whether Plaintiffs and the Class are entitled to damages, treble damages, or injunctive relief.

118. **Predominance**: Further, common questions of law and fact predominate over any individualized questions, and a class action is superior to individual litigation or any other available method to fairly and efficiently adjudicate the controversy. The damages available to individual Plaintiffs are insufficient to make individual lawsuits economically feasible.

119. **Superiority**: A class action is superior to other available methods for the fair and efficient adjudication of this controversy because joinder of all members is impracticable, the likelihood of individual Class members prosecuting separate claims is remote and individual members do not have a significant interest in individually controlling the prosecution of separate actions. No difficulty will be encountered in this case's management to preclude maintenance as a class action.

120. **Manageability**: The Class litigation will be manageable because all issues are identical, and individualized calculation of damages can be accomplished methodically by an expert via the use of data and information provided by HUB and its agents.

121. Plaintiffs and Class Members have suffered injury, harm, and damages because of

HUB's unlawful and wrongful conduct. Absent a class action, HUB will continue to maintain Plaintiffs' and Class Members' PII that could be subject to future breaches due to lax or non-existent cybersecurity measures, and such unlawful and improper conduct should not go unchecked nor remedied. Absent a class action, the Class Members will not be able to effectively litigate these claims and will suffer further harm and losses, as HUB will be allowed to continue such conduct with impunity and benefit from its unlawful conduct.

122. Likewise, particular issues under Rule 23(c)(4) are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include those set forth above.

123. HUB has acted on grounds that apply generally to the Class as a whole, so that Class certification, injunctive relief, and corresponding declaratory relief are appropriate on a Class-wide basis.

VI. CAUSES OF ACTION

COUNT I
NEGLIGENCE
(On behalf of Plaintiffs and the Class)

124. Plaintiffs re-allege and incorporate by reference paragraphs 1-123 as if fully set forth herein.

125. Plaintiffs' and the Class's PII was entrusted to Defendant. Defendant owed to Plaintiffs and the Class a duty to exercise reasonable care in handling and using the PII in its care and custody, including implementing industry-standard security procedures sufficient to reasonably protect the information from the Data Breach, and to promptly detect attempts at unauthorized access.

126. Defendant owed a duty of care to Plaintiffs and members of the Class because it was foreseeable that Defendant's failure to adequately safeguard their PII in accordance with state-of-the-art industry standards concerning data security would result in the compromise of that PII—just like the Data Breach that ultimately came to pass. Defendant acted with wanton and reckless disregard for the security and confidentiality of Plaintiffs' and the Class's PII by disclosing and providing access to this information to unauthorized third parties and by failing to properly supervise both the way the PII was stored, used, and exchanged, and those in its employ who were responsible for making that happen.

127. Defendant owed to Plaintiffs and members of the Class a duty to notify them within a reasonable timeframe of any breach to the security of their PII. Defendant also owed a duty to timely and accurately disclose to Plaintiffs and members of the Class the scope, nature, and occurrence of the Data Breach. This duty is required and necessary for Plaintiffs and the Class to take appropriate measures to protect their PII, to be vigilant in the face of an increased risk of harm, and to take other necessary steps to mitigate the harm caused by the Data Breach.

128. Defendant owed these duties to Plaintiffs and members of the Class because they are members of a well-defined, foreseeable, and probable class of individuals whom Defendant knew or should have known would suffer injury-in-fact from Defendant's inadequate security protocols. Defendant actively sought and obtained Plaintiffs' and the Class's PII.

129. Additionally, pursuant to the FTC Act, 15 U.S.C. § 45, Defendant had a duty to provide fair and adequate computer systems and data security practices to safeguard Plaintiffs' and the Class's PII.

130. Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as

Defendant, of failing to use reasonable measures to protect customers or, in this case, employees' PII. The FTC publications and orders promulgated pursuant to the FTC Act also form part of the basis of Defendant's duty to protect Plaintiffs' and the members of the Class's PII.

131. Defendant breached its respective duties to Plaintiffs and Class Members under the FTC Act by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard PII.

132. Defendant's duty to use reasonable care in protecting confidential data arose not only as a result of the statutes and regulations described above, but also because Defendant is bound by industry standards to protect confidential PII.

133. Defendant violated its duty under Section 5 of the FTC Act by failing to use reasonable measures to protect Plaintiffs' and the Class's PII and not complying with applicable industry standards as described in detail herein. Defendant's conduct was particularly unreasonable given the nature and amount of PII Defendant collected and stored and the foreseeable consequences of a data breach, including, specifically, the immense damages that would result to individuals in the event of a breach, which ultimately came to pass.

134. The harm that has occurred is the type of harm the FTC Act is intended to guard against. Indeed, the FTC has pursued numerous enforcement actions against businesses that, because of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiffs and the Class.

135. But for Defendant's wrongful and negligent breach of the duties owed to Plaintiffs and members of the Class, Plaintiffs and members of the Class would not have been injured.

136. The injury and harm suffered by Plaintiffs and members of the Class were the

reasonably foreseeable result of Defendant's breach of its duties. Defendant knew or should have known that it was failing to meet its duties and that its breach would cause Plaintiffs and members of the Class to suffer the foreseeable harms associated with the exposure of their PII.

137. Had Plaintiffs and the Class known that Defendant did not adequately protect their PII, Plaintiffs and members of the Class would not have allowed Defendant to access their PII.

138. As a direct and proximate result of Defendant's negligence, Plaintiffs and the Class have suffered harm, including loss of time and money resolving fraudulent charges; loss of time and money obtaining protections against future identity theft; lost control over the value of PII; harm resulting from damaged credit scores and information; and other harm resulting from the unauthorized use or threat of unauthorized use of stolen PII, entitling them to damages in an amount to be proven at trial.

139. The risk that unauthorized persons would attempt to gain access to the PII and misuse it was foreseeable. Given that Defendant held vast amounts of PII, it was inevitable that unauthorized individuals would attempt to access Defendant's databases containing the PII — whether by malware or otherwise.

140. PII is highly valuable, and Defendant knew, or should have known, the risk in obtaining, using, handling, emailing, and storing the PII of Plaintiffs and the Class and the importance of exercising reasonable care in handling it. Especially with multiple other businesses experiencing data breaches.

141. Defendant breached its duties by failing to exercise reasonable care in protecting the PII of Plaintiffs and the Class, supervising and monitoring its employees, agents, contractors, vendors, and suppliers, and in handling and securing the PII of Plaintiffs and the Class which

actually and proximately caused the Data Breach and Plaintiffs' and the Class's injury. Defendant further breached its duties by failing to provide reasonably timely notice of the Data Breach to Plaintiffs and members of the Class, which actually and proximately caused and exacerbated the harm from the Data Breach and Plaintiffs' and members of the Class's injuries-in-fact. As a direct and traceable result of Defendant's negligence and/or negligent supervision, Plaintiffs and the Class have suffered or will suffer damages, including monetary damages, increased risk of future harm, embarrassment, humiliation, frustration, and emotional distress.

142. Defendant's breach of their common-law duties to exercise reasonable care and their failures and negligence actually and proximately caused Plaintiffs and members of the Class actual, tangible, injury-in-fact and damages, including, without limitation, the theft of their PII by criminals, improper disclosure of their PII, lost benefit of their bargain, lost value of their PII, and lost time and money incurred to mitigate and remediate the effects of the Data Breach that resulted from and were caused by Defendant's negligence, which injury-in-fact and damages are ongoing, imminent, immediate, and which they continue to face.

COUNT II
UNJUST ENRICHMENT
(On behalf of Plaintiffs and the Class)

143. Plaintiffs re-allege and incorporate by reference paragraphs 1-123 as if fully set forth herein.

144. This claim is pleaded in the alternative to the breach of contract claim(s).

145. Plaintiffs and members of the Class conferred a benefit upon Defendant in in the form of their PII, which allowed Defendant to render services and make revenue therefrom.

146. Defendant appreciated or had knowledge of the benefits conferred upon it by Plaintiffs and the Class. Defendant also benefited from the receipt of Plaintiffs' and the Class's

PII, as this was used to facilitate the services it sold.

147. Under principles of equity and good conscience, Defendant should not be permitted to retain the full value of the benefit because Defendant failed to adequately protect their PII. Plaintiffs and the proposed Class would not have provided their PII to Defendant and/or a client of Defendant had they known Defendant would not adequately protect their PII.

148. Defendant should be compelled to disgorge into a common fund for the benefit of Plaintiffs and members of the Class all unlawful or inequitable proceeds received by them because of their misconduct and Data Breach.

COUNT III
INVASION OF PRIVACY
(On behalf of Plaintiffs and the Class)

149. Plaintiffs re-allege and incorporate by reference paragraphs 1-123 as if fully set forth herein.

150. Plaintiffs and Class Members had a legitimate expectation of privacy regarding their PII and were accordingly entitled to the protection of this information against disclosure to unauthorized third parties.

151. Defendant owed a duty to Plaintiffs and Class Member to keep their PII confidential.

152. Defendant affirmatively and recklessly disclosed Plaintiffs' and Class Members' PII to unauthorized third parties.

153. The unauthorized disclosure and/or acquisition (*i.e.*, theft) by a third party of Plaintiffs' and Class Members' PII is highly offensive to a reasonable person.

154. Defendant's reckless and negligent failure to protect Plaintiffs' and Class Members' PII constitutes an intentional interference with Plaintiffs' and the Class Members'

interest in solitude or seclusion, either as to their person or as to their private affairs or concerns, of a kind that would be highly offensive to a reasonable person.

155. Defendant's failure to protect Plaintiffs' and Class Members' PII acted with a knowing state of mind when it permitted the Data Breach because it knew its information security practices were inadequate.

156. Defendant knowingly did not notify Plaintiffs and Class Members in a timely fashion about the Data Breach.

157. Because Defendant failed to properly safeguard Plaintiffs' and Class Members' PII, Defendant had notice and knew that its inadequate cybersecurity practices would cause injury to Plaintiffs and the Class.

158. As a proximate result of Defendant's acts and omissions, Plaintiffs' and the Class Members' private and sensitive PII was stolen by a third party and is now available for disclosure and redisclosure without authorization, causing Plaintiffs and the Class to suffer damages.

159. Defendant's wrongful conduct will continue to cause great and irreparable injury to Plaintiffs and the Class since their PII is still maintained by Defendant with its inadequate cybersecurity system and policies.

160. Plaintiffs and Class Members have no adequate remedy at law for the injuries relating to Defendant's continued possession of their sensitive and confidential records. A judgment for monetary damages will not end Defendant's inability to safeguard Plaintiffs' and the Class's PII.

161. Plaintiffs, on behalf of herself and Class Members, seek injunctive relief to enjoin Defendant from further intruding into the privacy and confidentiality of Plaintiffs' and Class Members' PII.

162. Plaintiffs, on behalf of herself and Class Members, seek compensatory damages for Defendant's invasion of privacy, which includes the value of the privacy interest invaded by Defendant, the costs of future monitoring of their credit history for identity theft and fraud, plus prejudgment interest, and costs.

COUNT IV
INTRUSION UPON SECLUSION / INVASION OF PRIVACY
(On behalf of Plaintiffs and the Class)

163. Plaintiffs re-allege and incorporate by reference paragraphs 1-123 as if fully set forth herein.

164. Plaintiffs and Class Members maintain a privacy interest in their PII, which is private, confidential information that is also protected from disclosure by applicable laws set forth above.

165. Plaintiffs and Class Members' PII was contained, stored, and managed electronically in Defendant's records, computers, and databases that was intended to be secured from unauthorized access to third-parties because highly sensitive, confidential matters regarding Plaintiffs' and Class Members' identities were only shared with Defendant for the limited purpose of obtaining and paying for Defendant's services.

166. Additionally, Plaintiffs' and Class Members' PII is highly attractive to criminals who can nefariously use such PII for fraud, identity theft, and other crimes without the victims' knowledge and consent.

167. Defendant's disclosure of Plaintiffs' and Class Members' PII to unauthorized third parties as a result of its failure to adequately secure and safeguard their PII is offensive. Defendant's disclosure of Plaintiffs' and Class Members' PII to unauthorized third parties permitted the physical and electronic intrusion into private quarters where Plaintiffs' and Class

Members' PII was stored.

168. Plaintiffs and Class Members have been damaged by Defendant's conduct, including by incurring the harms and injuries arising from the Data Breach now and in the future.

COUNT V
BREACH OF IMPLIED CONTRACT
(On behalf of Plaintiffs and the Class)

169. Plaintiffs re-allege and incorporate by reference paragraphs 1-123 as if fully set forth herein.

170. Defendant acquired and maintained the PII of Plaintiffs and the Class including their Social Security numbers and other financial information to provide services.

171. In exchange, Defendant entered into implied contracts with Plaintiffs and the Class in which Defendant agreed to comply with its statutory and common law duties to protect Plaintiffs' and Class Members' PII and timely notify them of a Data Breach.

172. Based on Defendant's representations, legal obligations, and acceptance of Plaintiffs' and the Class Members' PII, Defendant had an implied duty to safeguard their PII through the use of reasonable industry standards.

173. Defendant breached the implied contracts by failing to safeguard Plaintiffs' and Class Members' PII and failing to provide them with timely and accurate notice of the Data Breach. Indeed, it took Defendant months to warn Plaintiffs and Class Member of their imminent risk of identity theft.

174. As a direct and proximate result of Defendant's breach of implied contract, Plaintiffs and the Class Members have suffered damages, including foreseeable consequential damages that Defendant knew about when it requested Plaintiffs' and the Class Members' PII.

175. Plaintiffs and the Class have suffered injuries as described herein, and are entitled

to actual and punitive damages, statutory damages, and reasonable attorneys' fees and costs, in an amount to be proven at trial.

COUNT VI
BREACH OF EXPRESS CONTRACT
(On behalf of Plaintiffs and the Class)

176. Plaintiffs re-allege and incorporate by reference paragraphs 1-123 as if fully set forth herein.

177. Defendant provides life insurance products to Plaintiffs and Class Members pursuant to the terms of its contracts, which all were a party to, including agreements regarding the handling of their confidential Personal Information in accordance with Defendant's policies, practices, and applicable law. Plaintiffs are not in possession of these contracts but upon information and belief these contracts are in the possession of Defendant. As consideration, Plaintiffs and Class Members paid money to Defendant and/or their insurers for life insurance products. Accordingly, Plaintiffs and Class Members paid Defendant to securely maintain and store their Personal Information. Defendant violated these contracts by failing to employ reasonable and adequate security measures to secure Plaintiffs' and Class Members' Personal Information and by disclosing it for purposes not required or permitted under the contracts.

178. Defendant's Privacy Policy is an agreement between Defendant and persons who provided their PII to Defendant, including Plaintiffs and Class Members.

179. Defendant's Privacy Policy provides detailed information about what types of and under what circumstances information will be collected and shared. It further promised to appropriately safeguard any PII it collects and to provide Plaintiffs and Class Members with a notification, to the extent required by applicable law, in the event of a data breach affecting their PII.

180. Plaintiffs and Class Members on the one hand and Defendant on the other formed a contract when Plaintiffs and Class Members provided their PII to Defendant subject to the Privacy Policy.

181. Plaintiffs and Class Members fully performed their obligations under the contract with Defendant.

182. Defendant breached its agreement with Plaintiffs and Class Members by failing to protect their PII. Specifically, Defendant (1) failed to use reasonable measures to protect that information; (2) disclosed that information to unauthorized third parties, in violation of the agreement; and (3) failed to provide an adequate and timely notice of the Breach as required by applicable law.

183. As a direct and proximate result of these breaches of contract, Plaintiffs and Class Members sustained actual losses and damages as described in detail above, including but not limited to that they did not get the benefit of the bargain for which they rendered valuable consideration to Defendant for its services.

184. Plaintiffs and Class Members have been damaged by Defendant's conduct, including by paying for data and cybersecurity protection that they did not receive, as well as by incurring the harms and injuries arising from the Data Breach now and in the future.

COUNT VII
BREACH OF CONFIDENCE
(On behalf of Plaintiffs and the Class)

185. Plaintiffs re-allege and incorporate by reference paragraphs 1-123 as if fully set forth herein.

186. At all times during Plaintiffs' and Class Members' relationship with Defendant, Defendant was fully aware of the confidential and sensitive nature of Plaintiffs' and Class

Members' Personal Information.

187. As alleged herein and above, Defendant's relationship with Plaintiffs and Class Members was governed by terms and expectations that Plaintiffs' and Class Members' Personal Information would be collected, stored, and protected in confidence, and would not be disclosed to unauthorized third parties.

188. Plaintiffs and Class Members provided their Personal Information to Defendant with the explicit and implicit understandings that Defendant would protect and not permit Personal Information to be disseminated to any unauthorized parties.

189. Plaintiffs and Class Members also provided their Personal Information to Defendant with the explicit and implicit understandings that Defendant would take precautions to protect such Personal Information from unauthorized disclosure.

190. Defendant voluntarily received in confidence Plaintiffs' and Class Members' Personal Information with the understanding that the Personal Information would not be disclosed or disseminated to the public or any unauthorized third parties.

191. Due to Defendant's failure to prevent, detect, or avoid the Data Breach from occurring by, inter alia, following industry standard information security practices to secure Plaintiffs' and Class Members' Personal Information, Plaintiffs and Class Members' Personal Information was disclosed and misappropriated to unauthorized third parties beyond Plaintiffs' and Class Members' confidence, and without their express permission.

192. As a direct and proximate cause of Defendant's actions and/or omissions, Plaintiffs and Class Members have suffered damages.

193. But for Defendant's disclosure of Plaintiffs' and Class Members' Personal Information in violation of the parties' understanding of confidence, their protected Personal

Information would not have been compromised, stolen, viewed, accessed, and used by unauthorized third parties. Defendant's Data Breach was the direct and legal cause of the theft of Plaintiffs' and Class Members' protected Personal Information, as well as the resulting damages.

194. The injury and harm Plaintiffs and Class Members suffered was the reasonably foreseeable result of Defendant's unauthorized disclosure of Plaintiffs' and Class Members' Personal Information.

195. As a direct and proximate result of Defendant's breaches of confidence, Plaintiffs and Class Members have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the compromise, publication, and/or theft of their Personal Information; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their Personal Information; (iv) lost opportunity costs associated with effort expended to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from medical fraud, financial fraud, and identity theft; (v) costs associated with placing freezes on credit reports; (vi) the continued risk to their Personal Information, which remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Personal Information of patients in its continued possession; and (vii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the Personal Information compromised as a result of the Data Breach for the remainder of the lives of Plaintiffs and Class Members.

196. As a direct and proximate result of Defendant's breaches of confidence, Plaintiffs and Class Members have suffered and will continue to suffer injury and/or harm.

COUNT VIII
BREACH OF THIRD-PARTY BENEFICIARY CONTRACT
(On behalf of Plaintiffs and the Class)

197. Plaintiffs re-allege and incorporate by reference paragraphs 1-123 as if fully set forth herein.

198. Upon information and belief, Defendant entered into contracts to provide insurance brokerage services to its clients including, upon information and belief, Plaintiffs' employer, which services included data security practices, procedures, and protocols sufficient to safeguard the PII that was to be entrusted to it.

199. Upon information and belief, these contracts are virtually identical.

200. These contracts were made expressly for the benefit of Plaintiffs and the Class, as it was their PII that Defendant agreed to receive and protect through its services. Thus, the benefit of collection and protection of the PII belonging to Plaintiffs and the Class was the direct and primary objective of the contracting parties.

201. Defendant knew that if it were to breach these contracts with its clients, the clients' employees, including Plaintiffs, would be harmed.

202. Defendant breached its contracts with its clients whose employees were affected by this Data Breach when it failed to use reasonable data security measures that could have prevented the Data Breach.

203. As foreseen, Plaintiffs and the Class were harmed by Defendant's failure to use reasonable data security measures to store highly sensitive personal information, including but not limited to, the continuous and substantial risk of harm through the loss of their PII.

204. Accordingly, Plaintiffs and the Class are entitled to damages in an amount to be determined at trial, along with costs and attorneys' fees incurred in this action.

COUNT IX
BREACH OF FIDUCIARY DUTY
(On behalf of Plaintiffs and the Class)

205. Plaintiffs re-allege and incorporate by reference paragraphs 1-123 as if fully set forth herein.

206. Given the relationship between Defendant and Plaintiffs and Class members, where Defendant became guardian of Plaintiffs' and Class members' PII, Defendant became a fiduciary by its undertaking and guardianship of the PII, to act primarily for Plaintiffs and Class members, (1) for the safeguarding of Plaintiffs and Class members' PII; (2) to timely notify Plaintiffs and Class members of a Data Breach and disclosure; and (3) to maintain complete and accurate records of what information (and where) Defendant did and does store.

207. Defendant has a fiduciary duty to act for the benefit of Plaintiffs and Class members upon matters within the scope of Defendant's relationship with them—especially to secure their PII.

208. Because of the highly sensitive nature of the PII, Plaintiffs and Class members (or their third-party agents) would not have entrusted Defendant, or anyone in Defendant's position, to retain their PII had they known the reality of Defendant's inadequate data security practices.

209. Defendant breached its fiduciary duties to Plaintiffs and Class members by failing to sufficiently encrypt or otherwise protect Plaintiffs' and Class members' PII.

210. Defendant also breached its fiduciary duties to Plaintiffs and Class members by failing to diligently discover, investigate, and give notice of the Data Breach in a reasonable and practicable period.

211. As a direct and proximate result of Defendant's breach of its fiduciary duties, Plaintiffs and Class members have suffered and will continue to suffer numerous injuries (as

detailed supra)

COUNT X
VIOLATIONS OF THE ILLINOIS CONSUMER FRAUD AND DECEPTIVE BUSINESS PRACTICES ACT ("CFA"), 815 ILL. COMP. STAT. §§ 505/1, *ET SEQ.*
(On behalf of Plaintiffs and the Class)

212. Plaintiffs re-allege and incorporate by reference paragraphs 1-123 as if fully set forth herein.

213. Plaintiffs and the Class are "consumers" as defined in 815 Ill. Comp. Stat. § 505/1(e). Plaintiffs, the Class, and Defendant are "persons" as defined in 815 Ill. Comp. Stat. § 505/1(c).

214. Defendant engaged in "trade" or "commerce," including the provision of services, as defined under 815 Ill. Comp. Stat. § 505/1(f). Defendant engages in the sale of "merchandise" (including services) as defined by 815 Ill. Comp. Stat. § 505/1(b) and (d).

215. Defendant engaged in deceptive and unfair acts and practices, misrepresentation, and the concealment and omission of material facts in connection with the sale and advertisement of their services in violation of the CFA, including: (i) failing to maintain adequate data security to keep Plaintiffs' and the Class Members' sensitive PII from being stolen by cybercriminals and failing to comply with applicable state and federal laws and industry standards pertaining to data security, including the FTC Act; (ii) failing to disclose or omitting materials facts to Plaintiffs and the Class regarding their lack of adequate data security and inability or unwillingness to properly secure and protect the PII of Plaintiffs and the Class; (iii) failing to disclose or omitting materials facts to Plaintiffs and the Class about Defendant's failure to comply with the requirements of relevant federal and state laws pertaining to the privacy and security of the PII of Plaintiffs and the Class; and (iv) failing to take proper action following the Data Breach to enact adequate privacy

and security measures and protect Plaintiffs' and the Class's PII and other PII from further unauthorized disclosure, release, data breaches, and theft.

216. These actions also constitute deceptive and unfair acts or practices because Defendant knew the facts about their inadequate data security and failure to comply with applicable state and federal laws and industry standards would be unknown to and not easily discoverable by Plaintiffs and the Class and defeat their reasonable expectations about the security of their PII.

217. Defendant intended that Plaintiffs and the Class rely on its deceptive and unfair acts and practices and the concealment and omission of material facts in connection with Defendant's offering of goods and services.

218. Defendant's wrongful practices were and are injurious to the public because those practices were part of Defendant's generalized course of conduct that applied to the Class. Plaintiffs and the Class have been adversely affected by Defendant's conduct and the public was and is at risk as a result thereof.

219. Defendant also violated 815 ILCS 505/2 by failing to immediately notify Plaintiffs and the Class of the nature and extent of the Data Breach pursuant to the Illinois PII Protection Act, 815 ILCS 530/1, et seq.

220. As a result of Defendant's wrongful conduct, Plaintiffs and the Class were injured in that they never would have provided their PII to Defendant, or purchased Defendant's services, had they known or been told that Defendant failed to maintain sufficient security to keep their PII from being hacked and taken and misused by others.

221. As a direct and proximate result of Defendant's violations of the CFA, Plaintiffs and the Class have suffered harm: (i) actual identity theft; (ii) the loss of the opportunity how their PII is used; (iii) the compromise, publication, and/or theft of their PII; (iv) out-of-pocket expenses

associated with the prevention, detection, and recovery from identity theft, and/or unauthorized use of their PII; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (vi) the continued risk to their PII, which remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fail to undertake appropriate and adequate measures to protect PII in their continued possession; and (vii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the PII compromised as a result of the Data Breach for the remainder of the lives of Plaintiffs and Class Members.

222. Pursuant to 815 Ill. Comp. Stat. § 505/10a(a), Plaintiffs and the Class seek actual and compensatory damages, injunctive relief, and court costs and attorneys' fees as a result of Defendant's violations of the CFA.

COUNT XI
DECLARATORY JUDGMENT
(On behalf of Plaintiffs and the Class)

223. Plaintiffs re-allege and incorporate by reference paragraphs 1-123 as if fully set forth herein.

224. Under the Declaratory Judgment Act, 28 U.S.C. § 2201, et seq., this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and to grant further necessary relief. Furthermore, the Court has broad authority to restrain acts that are tortious and violate the terms of the federal statutes described in this Complaint.

225. Defendant owes a duty of care to Plaintiffs and Class Members, which required it to adequately secure Plaintiffs' and Class Members' PII.

226. Defendant still possesses PII regarding Plaintiffs and Class Members.

227. Plaintiffs alleges that Defendant's data security measures remain inadequate. Furthermore, Plaintiffs continue to suffer injury as a result of the compromise of their PII and the risk remains that further compromises of their PII will occur in the future.

228. Under its authority pursuant to the Declaratory Judgment Act, this Court should enter a judgment declaring, among other things, the following:

k. Defendant owes a legal duty to secure the PII stored on its systems and within its network, and to timely notify victims of a data breach under the common law and Section 5 of the FTCA;

l. Defendant's existing security measures do not comply with its explicit or implicit contractual obligations and duties of care to provide reasonable security procedures and practices that are appropriate to protect PII; and

m. Defendant continues to breach this legal duty by failing to employ reasonable measures to secure the PII at issue.

229. This Court should also issue corresponding prospective injunctive relief requiring Defendant to employ adequate security protocols consistent with legal and industry standards to protect Plaintiffs' and Class Members' PII, including the following:

a. Order Defendant to provide lifetime credit monitoring and identity theft insurance to Plaintiffs and Class Members.

b. Order that, to comply with Defendant's explicit or implicit contractual obligations and duties of care, Defendant must implement and maintain reasonable security measures, including, but not limited to:

i. engaging third-party security auditors/penetration testers as well as

internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendant's systems on a periodic basis, and ordering Defendant to promptly correct any problems or issues detected by such third-party security auditors;

ii. engaging third-party security auditors and internal personnel to run automated security monitoring;

iii. auditing, testing, and training its security personnel regarding any new or modified procedures;

iv. segmenting its user applications by, among other things, creating firewalls and access controls so that if one area is compromised, hackers cannot gain access to other portions of Defendant's systems;

v. conducting regular database scanning and security checks;

vi. routinely and continually conducting internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach; and

vii. meaningfully educating Plaintiffs and Class Members about the threats they face with regard to the security of their PII, as well as the steps victims of the HUB Data Breach should take to protect themselves.

230. If an injunction is not issued, Plaintiffs will suffer irreparable injury and will lack an adequate legal remedy to prevent another data breach at HUB. The risk of another such breach is real, immediate, and substantial. If another breach at HUB occurs, Plaintiffs will not have an adequate remedy at law because many of the resulting injuries are not readily quantifiable.

231. The hardship to Plaintiffs if an injunction does not issue exceeds the hardship to

Defendant if an injunction is issued. Plaintiffs will likely be subjected to substantial, continued identity theft and other related damages if an injunction is not issued. On the other hand, the cost of Defendant's compliance with an injunction requiring reasonable prospective data security measures is relatively minimal, and Defendant has a pre-existing legal obligation to employ such measures.

232. Issuance of the requested injunction will not disserve the public interest. To the contrary, such an injunction would benefit the public by preventing a subsequent data breach at Defendant, thus preventing future injury to Plaintiffs and Class Members whose PII would be further compromised.

VII. PRAYER FOR RELIEF

Plaintiffs, on behalf of themselves and the Class, demand a jury trial on all claims so triable and request that the Court enter an order:

A. Certifying this case as a class action on behalf of Plaintiffs and the proposed Class, appointing Plaintiffs as class representatives, and appointing their counsel to represent the Class;

B. Awarding declaratory and other equitable relief as is necessary to protect the interests of Plaintiffs and the Class;

C. Awarding injunctive relief as is necessary to protect the interests of Plaintiffs and the Class;

D. Enjoining Defendant from further deceptive practices and making untrue statements about the Data Breach and the stolen PII;

E. Awarding Plaintiffs and the Class damages that include applicable compensatory, exemplary, punitive damages, and statutory damages, as allowed by law;

F. Awarding restitution and damages to Plaintiffs and the Class in an amount to be determined at trial;

G. Awarding attorneys' fees and costs, as allowed by law;

H. Awarding prejudgment and post-judgment interest, as provided by law;

I. Granting Plaintiffs and the Class leave to amend this complaint to conform to the evidence produced at trial; and

J. Granting such other or further relief as may be appropriate under the circumstances.

VIII. JURY DEMAND

Plaintiffs hereby demand that this matter be tried before a jury.

Dated: November 9, 2023

By: */s/ Raina C. Borrelli*

Raina Borrelli
Sam Strauss
TURKE & STRAUSS LLP
613 Williamson St., Suite 201
Madison, Wisconsin 53703-3515
Telephone: (608) 237-1775
Facsimile: (608) 509 4423
raina@turkestrauss.com
sam@turkestrauss.com

William B. Federman
FEDERMAN & SHERWOOD
10205 N. Pennsylvania Ave.
Oklahoma City, OK 73120
T: (405) 235-1560
F: (405) 239-2112
wbf@federmanlaw.com

John A. Yanchunis
Ra O. Amen
MORGAN & MORGAN
COMPLEX LITIGATION GROUP
201 North Franklin Street 7th Floor

Tampa, Florida 33602
T: (813) 223-5505
F: (813) 223-5402
jyanchunis@forthepeople.com
ramen@forthepeople.com

Mason A. Barney
Tyler J. Bean
SIRI & GLIMSTAD LLP
745 Fifth Avenue, Suite 500
New York, New York 10151
T: (212) 532-1091
mbarney@sirillp.com
tbean@sirillp.com

Attorneys for Plaintiffs and the Proposed Class

CERTIFICATE OF SERVICE

I, Raina C. Borrelli, hereby certify that I electronically filed the foregoing with the Clerk of the Court using the CM/ECF system, which will send notification of such filing to counsel of record via the ECF system.

DATED this 9th day of November, 2023.

By: */s/ Raina C. Borrelli*

Raina Borrelli (*pro hac vice*)
raina@turkestrauss.com
TURKE & STRAUSS LLP
613 Williamson St., Suite 201
Madison, Wisconsin 53703-3515
Telephone: (608) 237-1775
Facsimile: (608) 509 4423